

27

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 1817, AS REPORTED
OFFERED BY MR. COX OF CALIFORNIA**

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the "Department of Home-
3 land Security Authorization Act for Fiscal Year 2006".

4 SEC. 2. TABLE OF CONTENTS.

5 The table of contents for this Act is as follows:

Sec. 1. Short title.

Sec. 2. Table of contents.

TITLE I—AUTHORIZATION OF APPROPRIATIONS

Sec. 101. Department of Homeland Security.

Sec. 102. Customs and border protection; border patrol agents.

Sec. 103. Departmental management and operations.

Sec. 104. Critical infrastructure grants.

Sec. 105. Research and development.

Sec. 106. Border and transportation security.

Sec. 107. State and local terrorism preparedness.

Sec. 108. Immigration resources.

**TITLE II—TERRORISM PREVENTION, INFORMATION SHARING,
AND RISK ASSESSMENT**

Subtitle A—Terrorism Prevention

Sec. 201. Consolidated background check process.

**Subtitle B—Homeland Security Information Sharing and Analysis
Enhancement**

Sec. 211. Short title.

Sec. 212. Provision of terrorism-related information to private sector officials.

Sec. 213. Analytic expertise on the threats from biological agents and nuclear weapons.

Sec. 214. Alternative analysis of homeland security information.



- Sec. 215. Assignment of information analysis and infrastructure protection functions.
- Sec. 216. Coordination of homeland security threat analysis provided to non-Federal officials.
- Sec. 217. 9/11 Memorial Homeland Security Fellows Program.
- Sec. 218. Access to nuclear terrorism-related information.
- Sec. 219. Access of Assistant Secretary for Information Analysis to terrorism information.
- Sec. 220. Administration of the Homeland Security Information Network.
- Sec. 221. IAIP personnel recruitment.
- Sec. 222. Homeland Security Information Requirements.
- Sec. 223. Homeland Security Advisory System.
- Sec. 224. Use of open-source information.
- Sec. 225. Full and efficient use of open-source information.
- Sec. 226. Coordination with the intelligence community.
- Sec. 227. Consistency with applicable Federal laws.

TITLE III—DOMESTIC PREPAREDNESS AND PROTECTION

Subtitle A—Preparedness and Protection

- Sec. 301. National terrorism exercise program.
- Sec. 302. Technology development and transfer.
- Sec. 303. Review of antiterrorism acquisitions.
- Sec. 304. Center of Excellence for Border Security.
- Sec. 305. Requirements relating to the Container Security Initiative (CSI).
- Sec. 306. Security of maritime cargo containers.
- Sec. 307. Security plan for general aviation at Ronald Reagan Washington National Airport.
- Sec. 308. Interoperable communications assistance.
- Sec. 309. Report to Congress on implementation of recommendations regarding protection of agriculture.

Subtitle B—Department of Homeland Security Cybersecurity Enhancement

- Sec. 311. Short title.
- Sec. 312. Assistant Secretary for Cybersecurity.
- Sec. 313. Cybersecurity training programs and equipment.
- Sec. 314. Cybersecurity research and development.

Subtitle C—Security of public transportation systems

- Sec. 321. Security best practices.
- Sec. 322. Public awareness.

Subtitle D—Critical infrastructure prioritization

- Sec. 331. Critical infrastructure.
- Sec. 332. Security review.
- Sec. 333. Implementation report.
- Sec. 334. Protection of information.

TITLE IV—U.S. CUSTOMS AND BORDER PROTECTION AND U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

- Sec. 401. Establishment and implementation of cost accounting system; reports.
- Sec. 402. Report relating to One Face at the Border Initiative.



Sec. 403. Customs services.

Sec. 404. Sense of Congress on interpretation of textile and apparel provisions.

TITLE V—MISCELLANEOUS

Sec. 501. Border security and enforcement coordination and operations.

Sec. 502. GAO report to Congress.

Sec. 503. Plan to reduce wait times.

Sec. 504. Denial of transportation security card.

Sec. 505. Transfer of existing Customs Patrol Officers unit and establishment of new CPO units in the Bureau of Immigration and Customs Enforcement.

Sec. 506. Data collection on use of immigration consultants.

Sec. 507. Office for State and local government coordination.

Sec. 508. Authority of other Federal agencies unaffected.

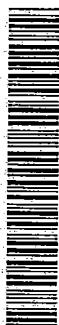
1 **TITLE I—AUTHORIZATION OF** 2 **APPROPRIATIONS**

3 **SEC. 101. DEPARTMENT OF HOMELAND SECURITY.**

4 There is authorized to be appropriated to the Sec-
5 retary of Homeland Security for the necessary expenses
6 of the Department of Homeland Security for fiscal year
7 2006, \$34,152,143,000.

8 **SEC. 102. CUSTOMS AND BORDER PROTECTION; BORDER** 9 **PATROL AGENTS.**

10 Of the amount authorized under section 101, there
11 is authorized to be appropriated for U.S. Customs and
12 Border Protection for fiscal year 2006, \$6,926,424,722,
13 of which \$1,839,075,277 is authorized for border security
14 and control between ports of entry, including for the hiring
15 of 2,000 full-time active-duty border patrol agents above
16 the number of such positions for which funds were allotted
17 for fiscal year 2005 (excluding any supplemental appro-
18 priations).



1 **SEC. 103. DEPARTMENTAL MANAGEMENT AND OPER-**
2 **ATIONS.**

3 Of the amount authorized under section 101, there
4 is authorized to be appropriated for fiscal year 2006 for
5 departmental management and operations, \$649,672,000,
6 of which—

7 (1) \$44,895,000 is authorized for the Depart-
8 ment of Homeland Security Regions Initiative;

9 (2) \$4,459,000 is authorized for Operation In-
10 tegration Staff; and

11 (3) \$56,278,000 is authorized for Office of Se-
12 curity initiatives.

13 **SEC. 104. CRITICAL INFRASTRUCTURE GRANTS.**

14 Of the amount authorized under section 101, there
15 is authorized to be appropriated for fiscal year 2006 for
16 grants and other assistance to improve critical infrastruc-
17 ture protection, \$465,000,000.

18 **SEC. 105. RESEARCH AND DEVELOPMENT.**

19 Of the amount authorized under section 101, there
20 are authorized to be appropriated for fiscal year 2006—

21 (1) \$76,573,000 to support chemical counter-
22 measure development activities of the Directorate of
23 Science and Technology;

24 (2) \$195,014,000 to support a nuclear detec-
25 tion office and related activities;



1 (3) \$19,000,000 for cybersecurity-related re-
2 search and development activities;

3 (4) \$10,000,000 for research and development
4 of technologies capable of countering threats posed
5 by man-portable air defense systems, including loca-
6 tion-based technologies and noncommercial aircraft-
7 based technologies; and

8 (5) \$10,600,000 for the activities of such direc-
9 torate conducted pursuant to subtitle G of title VIII
10 of the Homeland Security Act of 2002 (6 U.S.C.
11 441 et seq.).

12 **SEC. 106. BORDER AND TRANSPORTATION SECURITY.**

13 Of the amount authorized under section 101, there
14 are authorized to be appropriated for fiscal year 2006—

15 (1) \$826,913,000 for expenses related to
16 Screening Coordination and Operations of the Direc-
17 torate of Border and Transportation Security;

18 (2) \$100,000,000 for weapons of mass destruc-
19 tion detection technology of such directorate; and

20 (3) \$133,800,000 for the Container Security
21 Initiative of such directorate.

22 **SEC. 107. STATE AND LOCAL TERRORISM PREPAREDNESS.**

23 Of the amount authorized under section 101, there
24 are authorized to be appropriated for fiscal year 2006—



1 (1) \$40,500,000 for the activities of the Office
2 for Interoperability and Compatibility within the Di-
3 rectorate of Science and Technology pursuant to sec-
4 tion 7303 of the Intelligence Reform and Terrorism
5 Prevention Act of 2004 (6 U.S.C 194); and

6 (2) \$2,000,000,000 for grants to State and
7 local governments for terrorism preparedness award-
8 ed by the Office of State and Local Government Co-
9 ordination and Preparedness.

10 **SEC. 108. IMMIGRATION RESOURCES.**

11 Of the amount authorized under section 101, there
12 is authorized to be appropriated for fiscal year 2006 the
13 following:

14 (1) For the Immigration and Customs Enforce-
15 ment Legal Program, \$159,514,000, including for
16 the hiring of an additional 300 attorneys above the
17 number of such positions for which funds were allot-
18 ted for fiscal year 2005, and related training and
19 support costs.

20 (2) Sufficient sums for the hiring of an addi-
21 tional 300 adjudicators above the number of such
22 positions for which funds were allotted for fiscal
23 year 2005 to carry out the functions stated in sec-
24 tion 451(b) of the Homeland Security Act of 2002
25 (6 U.S.C. 271(b)), and related training and support



1 costs. The fees provided for in section 286(m) of the
2 Immigration and Nationality Act (8 U.S.C.
3 1356(m)) shall be adjusted in order to provide suffi-
4 cient sums for the hiring of the additional adjudica-
5 tors and for the related training and support costs
6 provided for in this paragraph.

7 **TITLE II—TERRORISM PREVEN-**
8 **TION, INFORMATION SHAR-**
9 **ING, AND RISK ASSESSMENT**
10 **Subtitle A—Terrorism Prevention**

11 **SEC. 201. CONSOLIDATED BACKGROUND CHECK PROCESS.**

12 (a) **REQUIREMENT.**—The Secretary of Homeland Se-
13 curity, in consultation with the Attorney General, shall es-
14 tablish a single process for conducting the security screen-
15 ing and background checks on individuals participating in
16 any of the programs identified under subsection (b).

17 (b) **INCLUDED PROGRAMS.**—The process established
18 under subsection (a) shall apply to the following programs:

19 (1) The Transportation Worker Identification
20 Credential.

21 (2) The security risk determination and related
22 background checks under section 5103a of title 49,
23 United States Code, performed by the Transpor-
24 tation Security Administration as part of the De-



1 partment of Transportation Hazardous Materials
2 Endorsement credentialing program.

3 (3) The Free and Secure Trade program.

4 (4) The NEXUS and SENTRI border crossing
5 programs.

6 (5) The Registered Traveler program of the
7 Transportation Security Administration.

8 (c) FEATURES OF PROCESS.—The process estab-
9 lished under subsection (a) shall include the following:

10 (1) A single submission of security screening in-
11 formation, including personal data and biometric in-
12 formation as appropriate, necessary to meet the se-
13 curity requirements of all applicable departmental
14 programs.

15 (2) An ability to submit such security screening
16 information at any location or through any process
17 approved by the Secretary with respect to any of the
18 applicable departmental programs.

19 (3) Acceptance by the Department of a security
20 clearance or other credential issued by a Federal
21 agency, to the extent that the security clearance
22 process of the agency satisfies requirements that are
23 at least as stringent as those of the applicable de-
24 partmental programs under subsection (b).



1 (4) Appropriate standards and procedures for
2 protecting individual privacy, confidentiality, record
3 retention, and addressing other concerns relating to
4 information security.

5 (d) DEADLINES.—The Secretary of Homeland Secu-
6 rity shall—

7 (1) submit a description of the process devel-
8 oped under subsection (a) to the appropriate con-
9 gressional committees (as defined in section 2 of the
10 Homeland Security Act of 2002 (6 U.S.C. 101)) by
11 not later than 6 months after the date of the enact-
12 ment of this Act; and

13 (2) begin implementing such process by not
14 later than 12 months after the date of the enact-
15 ment of this Act.

16 (e) INCLUSION OF OTHER PROGRAMS.—The Sec-
17 retary of Homeland Security shall review other existing
18 or developing Department of Homeland Security programs
19 that include security screening or background checks for
20 participating individuals, and report to the appropriate
21 congressional committees (as defined in section 2 of the
22 Homeland Security Act of 2002 (6 U.S.C. 101)) any rec-
23 ommendations for inclusion of such additional programs
24 in the consolidated screening process established under
25 this section.



1 (f) RELATIONSHIP TO OTHER LAWS.—(1) Nothing in
2 this section affects any statutory or regulatory require-
3 ment relating to the operation or standards of the pro-
4 grams described in subsection (b).

5 (2) Nothing in this section affects any statutory re-
6 quirement relating to title III of the Intelligence Reform
7 and Terrorism Prevention Act of 2004 (50 U.S.C. 435b
8 et seq.).

9 **Subtitle B—Homeland Security In-**
10 **formation Sharing and Analysis**
11 **Enhancement**

12 **SEC. 211. SHORT TITLE.**

13 This subtitle may be cited as the “Homeland Security
14 Information Sharing and Analysis Enhancement Act of
15 2005”.

16 **SEC. 212. PROVISION OF TERRORISM-RELATED INFORMA-**
17 **TION TO PRIVATE SECTOR OFFICIALS.**

18 Section 201(d) of the Homeland Security Act of 2002
19 (6 U.S.C. 121(d)) is amended by adding at the end the
20 following:

21 “(20) To require, in consultation with the As-
22 sistant Secretary for Infrastructure Protection, the
23 creation and routine dissemination of analytic re-
24 ports and products designed to provide timely and
25 accurate information that has specific relevance to



1 each of the Nation's private critical infrastructure
2 sectors (as identified in the national infrastructure
3 protection plan issued under paragraph (5)), to pri-
4 vate sector officials in each such sector who are re-
5 sponsible for protecting institutions within that sec-
6 tor from potential acts of terrorism and for miti-
7 gating the potential consequences of any such act.”.

8 **SEC. 213. ANALYTIC EXPERTISE ON THE THREATS FROM BI-**
9 **OLOGICAL AGENTS AND NUCLEAR WEAPONS.**

10 Section 201(d) of the Homeland Security Act of 2002
11 (6 U.S.C. 121(d)) is further amended by adding at the
12 end the following:

13 “(21) To ensure sufficient analytic expertise
14 within the Office of Information Analysis to create,
15 on an ongoing basis, products based on the analysis
16 of homeland security information, as defined in sec-
17 tion 892(f)(1), with specific reference to the threat
18 of terrorism involving the use of nuclear weapons
19 and biological agents to inflict mass casualties or
20 other catastrophic consequences on the population or
21 territory of the United States.”.



1 **SEC. 214. ALTERNATIVE ANALYSIS OF HOMELAND SECU-**
2 **RITY INFORMATION.**

3 (a) REQUIREMENT.—Subtitle A of title II of the
4 Homeland Security Act of 2002 (6 U.S.C. 121 et seq.)
5 is amended by adding at the end the following:

6 **“SEC. 203. ALTERNATIVE ANALYSIS OF HOMELAND SECU-**
7 **RITY INFORMATION.**

8 “The Secretary shall establish within the Department
9 a process and assign an individual or entity the responsi-
10 bility to ensure that, as appropriate, elements of the De-
11 partment conduct alternative analysis (commonly referred
12 to as ‘red-team analysis’) of homeland security informa-
13 tion, as that term is defined in section 892(f)(1), that re-
14 lates to potential acts of terrorism involving the use of
15 nuclear weapons or biological agents to inflict mass cas-
16 ualties or other catastrophic consequences on the popu-
17 lation or territory of the United States.”.

18 (b) CLERICAL AMENDMENT.—The table of contents
19 in section 1(b) of such Act is amended by inserting after
20 the item relating to section 202 the following:

“Sec. 203. Alternative analysis of homeland security information.”.

21 **SEC. 215. ASSIGNMENT OF INFORMATION ANALYSIS AND**
22 **INFRASTRUCTURE PROTECTION FUNCTIONS.**

23 Section 201(b) of the Homeland Security Act of 2002
24 (6 U.S.C. 121(b)) is amended by adding at the end the
25 following:



1 “(4) ASSIGNMENT OF SPECIFIC FUNCTIONS.—

2 The Under Secretary for Information Analysis and
3 Infrastructure Protection—

4 “(A) shall assign to the Assistant Sec-
5 retary for Information Analysis the responsi-
6 bility for performing the functions described in
7 paragraphs (1), (4), (7) through (14), (16), and
8 (18) of subsection (d);

9 “(B) shall assign to the Assistant Sec-
10 retary for Infrastructure Protection the respon-
11 sibility for performing the functions described
12 in paragraphs (2), (5), and (6) of subsection
13 (d);

14 “(C) shall assign to the Assistant Sec-
15 retary for Cybersecurity the primary authority
16 within the Department over the National Cyber
17 Security Division and the National Communica-
18 tions System, and, in coordination with other
19 relevant Federal agencies, the cybersecurity-re-
20 lated aspects of paragraphs (2), (3), (5), (6),
21 (15), and (17) of subsection (d);

22 “(D) shall ensure that the Assistant Sec-
23 retary for Information Analysis and the Assist-
24 ant Secretary for Infrastructure Protection both



1 perform the functions described in paragraphs
2 (3), (15), and (17) of subsection (d); and
3 “(E) may assign to each such Assistant
4 Secretary such other duties relating to such re-
5 sponsibilities as the Under Secretary may pro-
6 vide.”.

7 **SEC. 216. COORDINATION OF HOMELAND SECURITY**
8 **THREAT ANALYSIS PROVIDED TO NON-FED-**
9 **ERAL OFFICIALS.**

10 (a) IN GENERAL.—Title I of the Homeland Security
11 Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding
12 at the end the following:

13 **“SEC. 104. COORDINATION OF HOMELAND SECURITY**
14 **THREAT ANALYSIS PROVIDED TO NON-FED-**
15 **ERAL OFFICIALS.**

16 “(a) PRIMARY AUTHORITY.—Except as provided in
17 subsection (b), the Secretary shall be responsible for co-
18 ordinating all homeland security threat analysis to be pro-
19 vided to State and local government and tribal officials
20 and the private sector.

21 “(b) COORDINATION REQUIRED.—No Federal official
22 may disseminate any homeland security threat analysis to
23 State, local, tribal, or private sector officials without the
24 coordination of the Secretary or the Secretary’s designee
25 except—



1 “(1) in exigent circumstances under which it is
2 essential that the homeland security threat analysis
3 be communicated immediately; or

4 “(2) when such homeland security threat anal-
5 ysis is issued to State, local, or tribal law enforce-
6 ment officials for the purpose of assisting them in
7 any aspect of the administration of criminal justice.

8 “(c) DEFINITION.—(1) As used in this section, the
9 term ‘homeland security threat analysis’ means any infor-
10 mational product that is the result of evaluating informa-
11 tion, regardless of its source, in order to—

12 “(A) identify and assess the nature and scope
13 of terrorist threats to the homeland;

14 “(B) detect and identify threats of terrorism
15 against the United States; and

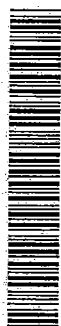
16 “(C) understand such threats in light of actual
17 and potential vulnerabilities of the territory of the
18 United States.

19 “(2) As defined in paragraph (1), the term ‘homeland
20 security threat analysis’ does not include—

21 “(A) any information that has not been proc-
22 essed, evaluated, or analyzed;

23 “(B) any information that is evaluated to create
24 any finished analytic product;

25 “(C) facts or summaries of facts;



1 “(D) reports of interviews; or

2 “(E) reports or other documents that merely
3 aggregate or summarize information derived from
4 multiple sources on the same or related topics.”.

5 (b) CLERICAL AMMENDMENT.—The table of contents
6 in section 1(b) of such Act is amended by inserting after
7 the item relating to section 103 the following:

“Sec. 104. Coordination of homeland security threat analysis provided to non-
Federal officials.”.

8 **SEC. 217. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS**
9 **PROGRAM.**

10 (a) ESTABLISHMENT OF PROGRAM.—Subtitle A of
11 title II of the Homeland Security Act of 2002 (6 U.S.C.
12 121 et seq.) is further amended by adding at the end the
13 following:

14 **“SEC. 204. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS**
15 **PROGRAM.**

16 “(a) ESTABLISHMENT.—

17 “(1) IN GENERAL.—The Secretary shall estab-
18 lish a fellowship program in accordance with this
19 section for the purpose of bringing State, local, trib-
20 al, and private sector officials to participate in the
21 work of the Homeland Security Operations Center in
22 order to become familiar with—

23 “(A) the mission and capabilities of that
24 Center; and



1 “(B) the role, programs, products, and
2 personnel of the Office of Information Analysis,
3 the Office of Infrastructure Protection, and
4 other elements of the Department responsible
5 for the integration, analysis, and dissemination
6 of homeland security information, as defined in
7 section 892(f)(1).

8 “(2) PROGRAM NAME.—The program under
9 this section shall be known as the 9/11 Memorial
10 Homeland Security Fellows Program.

11 “(b) ELIGIBILITY.—In order to be eligible for selec-
12 tion as a fellow under the program, an individual must—

13 “(1) have homeland security-related responsibil-
14 ities; and

15 “(2) possess an appropriate national security
16 clearance.

17 “(c) LIMITATIONS.—The Secretary—

18 “(1) may conduct up to 4 iterations of the pro-
19 gram each year, each of which shall be 90 days in
20 duration; and

21 “(2) shall ensure that the number of fellows se-
22 lected for each iteration does not impede the activi-
23 ties of the Center.

24 “(d) CONDITION.—As a condition of selecting an in-
25 dividual as a fellow under the program, the Secretary shall



1 require that the individual's employer agree to continue
2 to pay the individual's salary and benefits during the pe-
3 riod of the fellowship.

4 “(e) STIPEND.—During the period of the fellowship
5 of an individual under the program, the Secretary shall,
6 subject to the availability of appropriations, provide to the
7 individual a stipend to cover the individual's reasonable
8 living expenses during the period of the fellowship.”.

9 (b) CLERICAL AMENDMENT.—The table of contents
10 in section 1(b) of such Act is further amended by adding
11 at the end of the items relating to such subtitle the fol-
12 lowing:

“Sec. 204. 9/11 Memorial Homeland Security Fellows Program.”.

13 **SEC. 218. ACCESS TO NUCLEAR TERRORISM-RELATED IN-**
14 **FORMATION.**

15 Section 201(d) of the Homeland Security Act of 2002
16 (6 U.S.C. 121(d)) is further amended by adding at the
17 end the following:

18 “(22) To ensure that—

19 “(A) the Assistant Secretary for Informa-
20 tion Analysis receives promptly and without re-
21 quest all information obtained by any compo-
22 nent of the Department if that information re-
23 lates, directly or indirectly, to a threat of ter-
24 rorism involving the potential use of nuclear
25 weapons;



1 “(B) such information is—

2 “(i) integrated and analyzed com-
3 prehensively; and

4 “(ii) disseminated in a timely manner,
5 including to appropriately cleared Federal,
6 State, local, tribal, and private sector offi-
7 cials; and

8 “(C) such information is used to determine
9 what requests the Department should submit
10 for collection of additional information relating
11 to that threat.”.

12 **SEC. 219. ACCESS OF ASSISTANT SECRETARY FOR INFOR-**
13 **MATION ANALYSIS TO TERRORISM INFORMA-**
14 **TION.**

15 Section 201(d) of the Homeland Security Act of 2002
16 (6 U.S.C. 121(d)) is further amended by adding at the
17 end the following:

18 “(23) To ensure that the Assistant Secretary
19 for Information Analysis—

20 “(A) is routinely and without request given
21 prompt access to all terrorism-related informa-
22 tion collected by or otherwise in the possession
23 of any component of the Department, including
24 all homeland security information (as that term
25 is defined in section 892(f)(1)); and



1 “(B) to the extent technologically feasible
2 has direct access to all databases of any compo-
3 nent of the Department that may contain such
4 information.”.

5 **SEC. 220. ADMINISTRATION OF THE HOMELAND SECURITY**
6 **INFORMATION NETWORK.**

7 Section 201(d) of the Homeland Security Act of 2002
8 (6 U.S.C. 121(d)) is further amended by adding at the
9 end the following:

10 “(24) To administer the homeland security in-
11 formation network, including—

12 “(A) exercising primary responsibility for
13 establishing a secure nationwide real-time
14 homeland security information sharing network
15 for Federal, State, and local government agen-
16 cies and authorities, tribal officials, the private
17 sector, and other governmental and private en-
18 tities involved in receiving, analyzing, and dis-
19 tributing information related to threats to
20 homeland security;

21 “(B) ensuring that the information sharing
22 systems, developed in connection with the net-
23 work established under subparagraph (A), are
24 utilized and are compatible with, to the greatest
25 extent practicable, Federal, State, and local



1 government, tribal, and private sector
2 antiterrorism systems and protocols that have
3 been or are being developed; and

4 “(C) ensuring, to the greatest extent pos-
5 sible, that the homeland security information
6 network and information systems are integrated
7 and interoperable with existing private sector
8 technologies.”.

9 **SEC. 221. IAIP PERSONNEL RECRUITMENT.**

10 (a) IN GENERAL.—Chapter 97 of title 5, United
11 States Code, is amended by adding after section 9701 the
12 following:

13 **“§ 9702. Recruitment bonuses**

14 “(a) IN GENERAL.—Notwithstanding any provision
15 of chapter 57, the Secretary of Homeland Security, acting
16 through the Under Secretary for Information Analysis and
17 Infrastructure Protection, may pay a bonus to an indi-
18 vidual in order to recruit such individual for a position
19 that is primarily responsible for discharging the analytic
20 responsibilities specified in section 201(d) of the Home-
21 land Security Act of 2002 (6 U.S.C. 121(d)) and that—

22 “(1) is within the Directorate for Information
23 Analysis and Infrastructure Protection; and

24 “(2) would be difficult to fill in the absence of
25 such a bonus.



1 In determining which individuals are to receive bonuses
2 under this section, appropriate consideration shall be given
3 to the Directorate's critical need for linguists.

4 “(b) BONUS AMOUNT, FORM, ETC.—

5 “(1) IN GENERAL.—The amount of a bonus
6 under this section shall be determined under regula-
7 tions issued by the Secretary of Homeland Security,
8 with the concurrence of the Director of National In-
9 telligence, but may not exceed 50 percent of the an-
10 nual rate of basic pay of the position involved. The
11 Director of National Intelligence shall concur in
12 such regulations only if the amount of the bonus is
13 not disproportionate to recruitment bonuses offered
14 to intelligence analysts in other intelligence commu-
15 nity agencies.

16 “(2) FORM OF PAYMENT.—A bonus under this
17 section shall be paid in the form of a lump-sum pay-
18 ment and shall not be considered to be part of basic
19 pay.

20 “(3) COMPUTATION RULE.—For purposes of
21 paragraph (1), the annual rate of basic pay of a po-
22 sition does not include any comparability payment
23 under section 5304 or any similar authority.

24 “(c) SERVICE AGREEMENTS.—Payment of a bonus
25 under this section shall be contingent upon the employee



1 entering into a written service agreement with the Depart-
2 ment of Homeland Security. The agreement shall
3 include—

4 “(1) the period of service the individual shall be
5 required to complete in return for the bonus; and

6 “(2) the conditions under which the agreement
7 may be terminated before the agreed-upon service
8 period has been completed, and the effect of any
9 such termination.

10 “(d) ELIGIBILITY.—A bonus under this section may
11 not be paid to recruit an individual for—

12 “(1) a position to which an individual is ap-
13 pointed by the President, by and with the advice and
14 consent of the Senate;

15 “(2) a position in the Senior Executive Service
16 as a noncareer appointee (as defined under section
17 3132(a)); or

18 “(3) a position which has been excepted from
19 the competitive service by reason of its confidential,
20 policy-determining, policy-making, or policy-advo-
21 cating character.

22 “(e) TERMINATION.—The authority to pay bonuses
23 under this section shall terminate on September 30, 2008.



1 **“§ 9703. Reemployed annuitants**

2 “(a) IN GENERAL.—If an annuitant receiving an an-
3 nuity from the Civil Service Retirement and Disability
4 Fund becomes employed in a position within the Direc-
5 torate for Information Analysis and Infrastructure Protec-
6 tion of the Department of Homeland Security, the annu-
7 itant’s annuity shall continue. An annuitant so reemployed
8 shall not be considered an employee for the purposes of
9 chapter 83 or 84.

10 “(b) TERMINATION.—The exclusion pursuant to this
11 section of the Directorate for Information Analysis and
12 Infrastructure Protection from the reemployed annuitant
13 provisions of chapters 83 and 84 shall terminate 3 years
14 after the date of the enactment of this section, unless ex-
15 tended by the Secretary of Homeland Security. Any such
16 extension shall be for a period of 1 year and shall be re-
17 newable.

18 “(c) ANNUITANT DEFINED.—For purposes of this
19 section, the term ‘annuitant’ has the meaning given such
20 term under section 8331 or 8401, whichever is appro-
21 priate.

22 **“§ 9704. Regulations**

23 “The Secretary of Homeland Security, in consulta-
24 tion with the Director of the Office of Personnel Manage-
25 ment, may prescribe any regulations necessary to carry
26 out section 9702 or 9703.”.



1 (b) CLERICAL AMENDMENT.—The analysis for chap-
2 ter 97 of title 5, United States Code, is amended by add-
3 ing after the item relating to section 9701 the following:

“9702. Recruitment bonuses.
“9703. Reemployed annuitants.
“9704. Regulations.”.

4 **SEC. 222. HOMELAND SECURITY INFORMATION REQUIRE-**
5 **MENTS.**

6 (a) HOMELAND SECURITY INFORMATION REQUIRE-
7 MENTS.—The Joint Intelligence Community Council shall
8 advise the Director of National Intelligence with respect
9 to homeland security intelligence requirements.

10 (b) DESIGNATION OF MEMBERS.—The President
11 may designate officers of the United States Government
12 in addition to the members named in or designated under
13 section 101A(b) of the National Security Act to serve on
14 the Joint Intelligence Community Council in a capacity
15 limited to consideration of homeland security intelligence
16 requirements.

17 (c) PARTICIPATION IN NATIONAL INTELLIGENCE
18 COLLECTION REQUIREMENTS AND MANAGEMENT PROC-
19 ESSES.—The Secretary shall be a member of any Director
20 of National Intelligence-established interagency collection
21 and requirements management board that develops and
22 reviews national intelligence collection requirements in re-
23 sponse to Presidential intelligence guidelines.



1 **SEC. 223. HOMELAND SECURITY ADVISORY SYSTEM.**

2 (a) IN GENERAL.—Subtitle A of title II of the Home-
3 land Security Act of 2002 is further amended—

4 (1) in section 201(d)(7) (6 U.S.C. 121(d)(7))
5 by inserting “under section 205” after “System”;
6 and

7 (2) by adding at the end the following:

8 **“SEC. 205. HOMELAND SECURITY ADVISORY SYSTEM.**

9 “(a) REQUIREMENT.—The Under Secretary for In-
10 formation Analysis and Infrastructure Protection shall im-
11 plement a Homeland Security Advisory System in accord-
12 ance with this section to provide public advisories and
13 alerts regarding threats to homeland security, including
14 national, regional, local, and economic sector advisories
15 and alerts, as appropriate.

16 “(b) REQUIRED ELEMENTS.—The Under Secretary,
17 under the System—

18 “(1) shall include, in each advisory and alert re-
19 garding a threat, information on appropriate protec-
20 tive measures and countermeasures that may be
21 taken in response to the threat;

22 “(2) shall, whenever possible, limit the scope of
23 each advisory and alert to a specific region, locality,
24 or economic sector believed to be at risk; and

25 “(3) shall not, in issuing any advisory or alert,
26 use color designations as the exclusive means of



1 specifying the homeland security threat conditions
2 that are the subject of the advisory or alert.”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 1(b) of such Act is further amended by adding
5 at the end of the items relating to subtitle A of title II
6 the following:

“Sec. 205. Homeland Security Advisory System.”.

7 **SEC. 224. USE OF OPEN-SOURCE INFORMATION.**

8 Section 201(d) of the Homeland Security Act of 2002
9 (6 U.S.C. 121(d)) is further amended by adding at the
10 end the following:

11 “(25) To ensure that, whenever possible—

12 “(A) the Assistant Secretary for Informa-
13 tion Analysis utilizes open-source information
14 and produces reports and analytic products
15 based on such information that do not require
16 a national security classification under applica-
17 ble law; and

18 “(B) such unclassified open-source reports
19 are produced, to the extent consistent with the
20 protection of intelligence sources and methods
21 from unauthorized disclosure, contempora-
22 neously with reports or analytic products con-
23 cerning the same or similar information that
24 the Assistant Secretary for Information Anal-
25 ysis produces in a classified format.”.



1 **SEC. 225. FULL AND EFFICIENT USE OF OPEN-SOURCE IN-**
2 **FORMATION.**

3 (a) REQUIREMENT.—Subtitle A of title II of the
4 Homeland Security Act of 2002 (6 U.S.C. 121 et seq.)
5 is further amended by adding at the end the following:

6 **“SEC. 206. FULL AND EFFICIENT USE OF OPEN-SOURCE IN-**
7 **FORMATION.**

8 “The Under Secretary shall ensure that, in meeting
9 their analytic responsibilities under section 201(d) and in
10 formulating requirements for collection of additional infor-
11 mation, the Assistant Secretary for Information Analysis
12 and the Assistant Secretary for Infrastructure Protection
13 make full and efficient use of open-source information
14 wherever possible.”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of such Act is further amended by inserting
17 after the item relating to section 205 the following:

“Sec. 206. Full and efficient use of open-source information.”.

18 **SEC. 226. COORDINATION WITH THE INTELLIGENCE COM-**
19 **MUNITY.**

20 Section 201 of the Homeland Security Act of 2002
21 (6 U.S.C. 121) is amended by adding at the end the fol-
22 lowing:

23 “(h) COORDINATION WITH THE INTELLIGENCE COM-
24 MUNITY.—The Under Secretary shall ensure that, as to
25 the responsibilities specified in subsection (d), the Assist-



1 ant Secretary for Information Analysis serves as the offi-
2 cial responsible for coordinating, as appropriate, with ele-
3 ments of the intelligence community.”.

4 **SEC. 227. CONSISTENCY WITH APPLICABLE FEDERAL LAWS.**

5 Unless otherwise expressly stated in this subtitle, the
6 Secretary of Homeland Security shall ensure that all ac-
7 tivities carried out under this subtitle are consistent with
8 any applicable Federal laws relating to information policy
9 of Federal agencies.

10 **TITLE III—DOMESTIC PRE-**
11 **PAREDNESS AND PROTEC-**
12 **TION**

13 **Subtitle A—Preparedness and**
14 **Protection**

15 **SEC. 301. NATIONAL TERRORISM EXERCISE PROGRAM.**

16 (a) IN GENERAL.—Section 430(c) of the Homeland
17 Security Act of 2002 (6 U.S.C. 238) is amended by strik-
18 ing “and” after the semicolon at the end of paragraph
19 (8), by striking the period at the end of paragraph (9)
20 and inserting “; and”, and by adding at the end the fol-
21 lowing:

22 “(10) designing, developing, performing, and
23 evaluating exercises at the national, State, terri-
24 torial, regional, local, and tribal levels of government
25 that incorporate government officials, emergency re-



1 sponse providers, public safety agencies, the private
2 sector, international governments and organizations,
3 and other appropriate entities to test the Nation's
4 capability to prevent, prepare for, respond to, and
5 recover from threatened or actual acts of ter-
6 rorism.”.

7 (b) NATIONAL TERRORISM EXERCISE PROGRAM.—

8 (1) ESTABLISHMENT OF PROGRAM.—Title VIII
9 of the Homeland Security Act of 2002 (Public Law
10 107–296) is amended by adding at the end the fol-
11 lowing new subtitle:

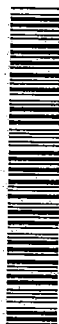
12 **“Subtitle J—Terrorism**
13 **Preparedness Exercises**

14 “SEC. 899a. NATIONAL TERRORISM EXERCISE PROGRAM.

15 “(a) IN GENERAL.—The Secretary, through the Of-
16 fice for Domestic Preparedness, shall establish a National
17 Terrorism Exercise Program for the purpose of testing
18 and evaluating the Nation's capabilities to prevent, pre-
19 pare for, respond to, and recover from threatened or ac-
20 tual acts of terrorism that—

21 “(1) enhances coordination for terrorism pre-
22 paredness between all levels of government, emer-
23 gency response providers, international governments
24 and organizations, and the private sector;

25 “(2) is—



1 “(A) multidisciplinary in nature, including,
2 as appropriate, information analysis and
3 cybersecurity components;

4 “(B) as realistic as practicable and based
5 on current risk assessments, including credible
6 threats, vulnerabilities, and consequences;

7 “(C) carried out with the minimum degree
8 of notice to involved parties regarding the tim-
9 ing and details of such exercises, consistent
10 with safety considerations;

11 “(D) evaluated against performance meas-
12 ures and followed by corrective action to solve
13 identified deficiencies; and

14 “(E) assessed to learn best practices,
15 which shall be shared with appropriate Federal,
16 State, territorial, regional, local, and tribal per-
17 sonnel, authorities, and training institutions for
18 emergency response providers; and

19 “(3) assists State, territorial, local, and tribal
20 governments with the design, implementation, and
21 evaluation of exercises that—

22 “(A) conform to the requirements of para-
23 graph (2); and

24 “(B) are consistent with any applicable
25 State homeland security strategy or plan.



1 “(b) NATIONAL LEVEL EXERCISES.—The Secretary,
2 through the National Terrorism Exercise Program, shall
3 perform on a periodic basis national terrorism prepared-
4 ness exercises for the purposes of—

5 “(1) involving top officials from Federal, State,
6 territorial, local, tribal, and international govern-
7 ments, as the Secretary considers appropriate;

8 “(2) testing and evaluating, in coordination
9 with the Attorney General, the Nation’s capability to
10 detect, disrupt, and prevent threatened or actual
11 catastrophic acts of terrorism, especially those in-
12 volving weapons of mass destruction; and

13 “(3) testing and evaluating the Nation’s readi-
14 ness to respond to and recover from catastrophic
15 acts of terrorism, especially those involving weapons
16 of mass destruction.

17 “(c) CONSULTATION WITH FIRST RESPONDERS.—In
18 implementing the responsibilities described in subsections
19 (a) and (b), the Secretary shall consult with a geographic
20 (including urban and rural) and substantive cross section
21 of governmental and nongovernmental first responder dis-
22 ciplines, including as appropriate—

23 “(1) Federal, State, and local first responder
24 training institutions;



1 “(2) representatives of emergency response pro-
2 viders; and

3 “(3) State and local officials with an expertise
4 in terrorism preparedness.”.

5 (2) CLERICAL AMENDMENT.—The table of con-
6 tents in section 1(b) of such Act is amended by add-
7 ing at the end of the items relating to title VIII the
8 following:

 “Subtitle J—Terrorism Preparedness Exercises

 “Sec. 899a. National terrorism exercise program.”.

9 (c) TOPOFF PREVENTION EXERCISE.—No later
10 than one year after the date of enactment of this Act, the
11 Secretary of Homeland Security shall design and carry out
12 a national terrorism prevention exercise for the purposes
13 of—

14 (1) involving top officials from Federal, State,
15 territorial, local, tribal, and international govern-
16 ments as the Secretary considers appropriate; and

17 (2) testing and evaluating, in coordination with
18 the Attorney General, the Nation’s capability to de-
19 tect, disrupt, and prevent threatened or actual cata-
20 strophic acts of terrorism, especially those involving
21 weapons of mass destruction.



1 **SEC. 302. TECHNOLOGY DEVELOPMENT AND TRANSFER.**

2 (a) ESTABLISHMENT OF TECHNOLOGY CLEARING-
3 HOUSE.—Not later than 90 days after the date of enact-
4 ment of this Act, the Secretary shall complete the estab-
5 lishment of the Technology Clearinghouse under section
6 313 of the Homeland Security Act of 2002.

7 (b) TRANSFER PROGRAM.—Section 313 of the Home-
8 land Security Act of 2002 (6 U.S.C. 193) is amended—

9 (1) by adding at the end of subsection (b) the
10 following new paragraph:

11 “(6) The establishment of a homeland security
12 technology transfer program to facilitate the identi-
13 fication, modification, and commercialization of tech-
14 nology and equipment for use by Federal, State, and
15 local governmental agencies, emergency response
16 providers, and the private sector to prevent, prepare
17 for, or respond to acts of terrorism.”;

18 (2) by redesignating subsection (c) as sub-
19 section (e); and

20 (3) by inserting after subsection (b) the fol-
21 lowing new subsections:

22 “(c) ELEMENTS OF THE TECHNOLOGY TRANSFER
23 PROGRAM.—The activities of the program described in
24 subsection (b)(6) shall include—

25 “(1) identifying available technologies that have
26 been, or are in the process of being, developed, test-

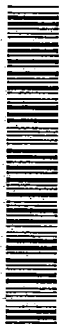


1 ed, evaluated, or demonstrated by the Department,
2 other Federal agencies, the private sector, or foreign
3 governments and international organizations, and re-
4 viewing whether such technologies may be useful in
5 assisting Federal, State, and local governmental
6 agencies, emergency response providers, or the pri-
7 vate sector to prevent, prepare for, or respond to
8 acts of terrorism; and

9 “(2) communicating to Federal, State, and local
10 governmental agencies, emergency response pro-
11 viders, or the private sector the availability of such
12 technologies for antiterrorism use, as well as the
13 technology’s specifications, satisfaction of appro-
14 priate standards, and the appropriate grants avail-
15 able from the Department to purchase such tech-
16 nologies;

17 “(d) RESPONSIBILITIES OF UNDER SECRETARY FOR
18 SCIENCE AND TECHNOLOGY.—In support of the activities
19 described in subsection (c), the Under Secretary for
20 Science and Technology shall—

21 “(1) conduct or support, based on the Depart-
22 ment’s current risk assessments of terrorist threats,
23 research, development, demonstrations, tests, and
24 evaluations, as appropriate, of technologies identified
25 under subparagraph (c)(1), including of any nec-



1 necessary modifications to such technologies for
2 antiterrorism use;

3 “(2) ensure that the technology transfer activi-
4 ties throughout the Directorate of Science and Tech-
5 nology are coordinated, including the technology
6 transfer aspects of projects and grants awarded to
7 the private sector and academia;

8 “(3) consult with the other Under Secretaries
9 of the Department and the Director of the Office for
10 Domestic Preparedness, on an ongoing basis;

11 “(4) consult with Federal, State, and local
12 emergency response providers;

13 “(5) consult with government agencies and
14 standards development organizations as appropriate;

15 “(6) enter into agreements and coordinate with
16 other Federal agencies, foreign governments, and
17 national and international organizations as the Sec-
18 retary determines appropriate, in order to maximize
19 the effectiveness of such technologies or to facilitate
20 commercialization of such technologies;

21 “(7) consult with existing technology transfer
22 programs and Federal and State training centers
23 that research, develop, test, evaluate, and transfer
24 military and other technologies for use by emergency
25 response providers; and



1 “(8) establish a working group in coordination
2 with the Secretary of Defense to advise and assist
3 the technology clearinghouse in the identification of
4 military technologies that are in the process of being
5 developed, or are developed, by the Department of
6 Defense or the private sector, which may include—

7 “(A) representatives from the Department
8 of Defense or retired military officers;

9 “(B) nongovernmental organizations or
10 private companies that are engaged in the re-
11 search, development, testing, or evaluation of
12 related technologies or that have demonstrated
13 prior experience and success in searching for
14 and identifying technologies for Federal agen-
15 cies;

16 “(C) Federal, State, and local emergency
17 response providers; and

18 “(D) to the extent the Secretary considers
19 appropriate, other organizations, other inter-
20 ested Federal, State, and local agencies, and
21 other interested persons.”.

22 (c) REPORT.—Not later than 1 year after the date
23 of enactment of this Act, the Under Secretary for Science
24 and Technology shall transmit to the Congress a descrip-
25 tion of the progress the Department has made in imple-



1 menting the provisions of section 313 of the Homeland
2 Security Act of 2002, as amended by this Act, including
3 a description of the process used to review unsolicited pro-
4 posals received as described in subsection (b)(3) of such
5 section.

6 (d) SAVINGS CLAUSE.—Nothing in this section (in-
7 cluding the amendments made by this section) shall be
8 construed to alter or diminish the effect of the limitation
9 on the authority of the Secretary of Homeland Security
10 under section 302(4) of the Homeland Security Act of
11 2002 (6 U.S.C. 182(4)) with respect to human health-re-
12 lated research and development activities.

13 **SEC. 303. REVIEW OF ANTITERRORISM ACQUISITIONS.**

14 (a) STUDY.—The Secretary of Homeland Security
15 shall conduct a study of all Department of Homeland Se-
16 curity procurements, including ongoing procurements and
17 anticipated procurements, to—

18 (1) identify those that involve any product,
19 equipment, service (including support services), de-
20 vice, or technology (including information tech-
21 nology) that is being designed, developed, modified,
22 or procured for the specific purpose of preventing,
23 detecting, identifying, or deterring acts of terrorism
24 or limiting the harm such acts might otherwise
25 cause; and



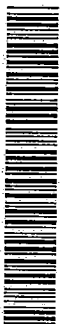
1 (2) assess whether such product, equipment,
2 service (including support services), device, or tech-
3 nology is an appropriate candidate for the litigation
4 and risk management protections of subtitle G of
5 title VIII of the Homeland Security Act of 2002.

6 (b) SUMMARY AND CLASSIFICATION REPORT.—Not
7 later than 180 days after the date of enactment of this
8 Act, the Secretary shall transmit to the Congress a
9 report—

10 (1) describing each product, equipment, service
11 (including support services), device, and technology
12 identified under subsection (a) that the Secretary
13 believes would be an appropriate candidate for the
14 litigation and risk management protections of sub-
15 title G of title VIII of the Homeland Security Act
16 of 2002;

17 (2) listing each such product, equipment, serv-
18 ice (including support services), device, and tech-
19 nology in order of priority for deployment in accord-
20 ance with current terrorism risk assessment infor-
21 mation; and

22 (3) setting forth specific actions taken, or to be
23 taken, to encourage or require persons or entities
24 that sell or otherwise provide such products, equip-
25 ment, services (including support services), devices,



1 and technologies to apply for the litigation and risk
2 management protections of subtitle G of title VIII of
3 the Homeland Security Act of 2002, and to ensure
4 prioritization of the Department's review of such
5 products, equipment, services, devices, and tech-
6 nologies under such Act in accordance with the
7 prioritization set forth in paragraph (2) of this sub-
8 section.

9 **SEC. 304. CENTER OF EXCELLENCE FOR BORDER SECU-**
10 **RITY.**

11 The Secretary of Homeland Security shall establish
12 a university-based Center of Excellence for Border Secu-
13 rity following the merit-review processes and procedures
14 and other limitations that have been established for select-
15 ing and supporting University Programs Centers of Excel-
16 lence. The Center shall prioritize its activities on the basis
17 of risk to address the most significant threats,
18 vulnerabilities, and consequences posed by the Nation's
19 borders and border control systems. The activities should
20 include the conduct of research, the examination of exist-
21 ing and emerging border security technology and systems,
22 and the provision of education, technical, and analytical
23 assistance for the Department of Homeland Security to
24 effectively secure the Nation's borders.



1 **SEC. 305. REQUIREMENTS RELATING TO THE CONTAINER**
2 **SECURITY INITIATIVE (CSI).**

3 (a) DESIGNATION OF NEW FOREIGN SEAPORTS.—

4 The Secretary of Homeland Security may designate a for-
5 eign seaport as a participating seaport in the Container
6 Security Initiative program on or after the date of the en-
7 actment of this Act if the Secretary—

8 (1) determines, based on a foreign port assess-
9 ment carried out under section 70108(a) of title 46,
10 United States Code, or such other risk assessment
11 that the Secretary may perform, and a cost-benefit
12 analysis, that the benefits of designating such sea-
13 port as a participating seaport outweigh the cost of
14 expanding the program to such seaport; and

15 (2) enters into an agreement with the foreign
16 government of such seaport, in consultation with the
17 Department of State and other appropriate Federal
18 agencies to—

19 (A) establish security criteria to identify
20 the potential compromise by terrorists or ter-
21 rorist weapons of maritime cargo containers
22 bound for the United States based on advance
23 information; and

24 (B) screen or inspect such maritime cargo
25 containers for potential compromise by terror-



1 ists or terrorist weapons prior to shipment to
2 the United States.

3 (b) DEPLOYMENT OF INSPECTION EQUIPMENT TO
4 NEW CSI PARTICIPATING SEAPORTS.—

5 (1) DEPLOYMENT.—The Secretary may—

6 (A) loan or otherwise provide nonintrusive
7 inspection equipment for maritime cargo con-
8 tainers, on a nonreimbursable basis, at a sea-
9 port designated under subsection(a); and

10 (B) provide training for personnel at a sea-
11 port designated under subsection (a) to operate
12 the nonintrusive inspection equipment.

13 (2) ADDITIONAL REQUIREMENTS.—

14 (A) CAPABILITY REQUIREMENTS AND OP-
15 ERATING PROCEDURES.—The Secretary shall
16 establish technical capability requirements and
17 standard operating procedures for nonintrusive
18 inspection equipment described in paragraph
19 (1), consistent with any standards established
20 by the Secretary under section 70116 of title 46
21 United States Code.

22 (B) AGREEMENT REQUIRED.—The Sec-
23 retary shall require each CSI port to agree to
24 operate such equipment in accordance with re-
25 quirements and procedures established under



1 subparagraph (A) as a condition for receiving
2 the equipment and training under paragraph
3 (1).

4 (c) DEPLOYMENT OF PERSONNEL TO NEW CSI
5 PORTS; REEVALUATION OF PERSONNEL AT ALL CSI
6 PORTS.—

7 (1) DEPLOYMENT.—The Secretary shall deploy
8 United States Customs and Border Protection per-
9 sonnel to each seaport designated under subsection
10 (a) with respect to which the Secretary determines
11 that the deployment is necessary to successfully im-
12 plement the requirements of CSI at the port.

13 (2) REEVALUATION.—The Secretary shall peri-
14 odically review relevant risk assessment information
15 with respect to each seaport at which personnel are
16 deployed under paragraph (1) to assess whether or
17 not continued deployment of such personnel, in
18 whole or in part, is necessary to success fully imple-
19 ment the requirements of CSI at the port.

20 (d) INSPECTION AND SCREENING AT UNITED
21 STATES PORTS OF ENTRY.—Cargo containers arriving at
22 a United States port of entry from a CSI port shall under-
23 go the same level of inspection and screening for potential
24 compromise by terrorists or terrorist weapons as cargo
25 containers arriving at a United States port of entry from



1 a foreign seaport that is not participating in CSI unless
2 the containers were initially inspected at the CSI port at
3 the request of personnel deployed under subsection (c) and
4 such personnel verify and electronically record that the in-
5 spection indicates that the containers have not been com-
6 promised by terrorists or terrorist weapons.

7 **SEC. 306. SECURITY OF MARITIME CARGO CONTAINERS.**

8 (a) STANDARDS AND REGULATIONS.—

9 (1) STANDARDS.—Not later than 180 days
10 after the date of the enactment of this Act, the Sec-
11 retary of Homeland Security shall establish stand-
12 ards and procedures for securing maritime cargo
13 containers relating to obligation to seal, recording of
14 seal changes, modal changes, seal placement, ocean
15 carrier seal verification, and addressing seal anoma-
16 lies. These standards shall include the standards for
17 seals and locks as required under paragraph (3) of
18 subsection (b) of section 70116 of title 46, United
19 States Code.

20 (2) REGULATIONS.—No later than 90 days
21 after completion of the requirements in subsection
22 (a), the Secretary of Homeland Security shall issue
23 regulations for the security of maritime cargo con-
24 tainers consistent with the standards developed in
25 subsection (a).



1 (b) INTERNATIONAL AGREEMENTS.—The Secretary,
2 in consultation with the Department of State, Department
3 of Commerce, Department of Treasury, Office of the
4 United States Trade Representative, and other appropriate Federal agencies, shall seek to enter into agreements with foreign countries and international organizations to establish standards for the security of maritime cargo containers moving within the intermodal transportation system that, to the maximum extent practicable,
5 meet the requirements of subsection (a).

11 (c) CONTAINER TARGETING STRATEGY.—The Secretary shall develop a strategy to improve the ability of
12 the Department of Homeland Security to use advance
13 cargo information to identify anomalies in such information to determine whether such cargo poses a security risk.
14 The strategy shall include a method of contacting shippers
15 to verify or explain any anomalies discovered in such information.

19 (d) CONTAINER SECURITY DEMONSTRATION PROGRAM.—
20

21 (1) PROGRAM.—The Secretary is authorized to
22 establish and carry out a demonstration program
23 that integrates radiation detection equipment with
24 other types of nonintrusive inspection equipment at



1 an appropriate United States seaport, as determined
2 by the Secretary.

3 (2) REQUIREMENT.—The demonstration pro-
4 gram shall also evaluate ways to strengthen the ca-
5 pability of Department of Homeland Security per-
6 sonnel to analyze cargo inspection data and ways to
7 improve the transmission of inspection data between
8 appropriate entities within the Department of
9 Homeland Security.

10 (e) COORDINATION AND CONSOLIDATION OF CON-
11 TAINER SECURITY PROGRAMS.—The Secretary shall co-
12 ordinate all programs that enhance the security of mari-
13 time cargo, and, to the extent practicable, consolidate Op-
14 eration Safe Commerce, the Smart Box Initiative, and
15 similar programs that evaluate security enhancements for
16 maritime cargo containers, to achieve enhanced coordina-
17 tion and efficiency. The Secretary shall report to the ap-
18 propriate congressional committees (as that term is de-
19 fined in section 2 of the Homeland Security Act of 2002
20 (6 U.S.C. 101) before consolidating any program men-
21 tioned in this subsection.



1 **SEC. 307. SECURITY PLAN FOR GENERAL AVIATION AT**
2 **RONALD REAGAN WASHINGTON NATIONAL**
3 **AIRPORT.**

4 Not later than 60 days after the date of enactment
5 of this Act, the Secretary of Homeland Security shall im-
6 plement section 823(a) of the Vision 100—Century of
7 Aviation Reauthorization Act (49 U.S.C. 41718 note; 117
8 Stat. 2595).

9 **SEC. 308. INTEROPERABLE COMMUNICATIONS ASSIST-**
10 **ANCE.**

11 (a) **FINDINGS.**—The Congress finds the following:

12 (1) The 9/11 Commission determined that the
13 inability of first responders to communicate effec-
14 tively on September 11, 2001 was a critical obstacle
15 to an effective multi-jurisdictional response.

16 (2) Many jurisdictions across the country still
17 experience difficulties communicating that may con-
18 tribute to confusion, delays, or added risks when re-
19 sponding to an emergency.

20 (3) During fiscal year 2004, the Office for Do-
21 mestic Preparedness awarded over \$834,000,000 for
22 2,912 projects through Department of Homeland
23 Security grant programs for the purposes of improv-
24 ing communications interoperability.

25 (4) Interoperable communications systems are
26 most effective when designed to comprehensively ad-



1 dress, on a regional basis, the communications of all
2 types of public safety agencies, first responder dis-
3 ciplines, and State and local government facilities.

4 (5) Achieving communications interoperability
5 is complex due to the extensive training, system
6 modifications, and agreements among the different
7 jurisdictions that are necessary to implement effec-
8 tive communications systems.

9 (6) The Congress authorized the Department of
10 Homeland Security to create an Office for Interoper-
11 ability and Compatibility in the Intelligence Reform
12 and Terrorism Prevention Act of 2004 to, among
13 other things, establish a comprehensive national ap-
14 proach, coordinate federal activities, accelerate the
15 adoption of standards, and encourage research and
16 development to achieve interoperable communica-
17 tions for first responders.

18 (7) The Office for Interoperability and Compat-
19 ibility includes the SAFECOM Program that serves
20 as the umbrella program within the Federal govern-
21 ment to improve public safety communications inter-
22 operability, and has developed the RAPIDCOM pro-
23 gram, the Statewide Communications Interoper-
24 ability Planning Methodology, and a Statement of
25 Requirements to provide technical, planning, and



1 purchasing assistance for Federal departments and
2 agencies, State and local governments, and first re-
3 sponders.

4 (b) SENSE OF CONGRESS.—It is the sense of the
5 Congress that the Department of Homeland Security
6 should implement as expeditiously as possible the initia-
7 tives assigned to the Office for Interoperability and Com-
8 patibility under section 7303 of the Intelligence Reform
9 and Terrorism Prevention Act of 2004 (6 U.S.C. 194),
10 including specifically the following:

11 (1) Establishing a comprehensive national ap-
12 proach to achieving public safety interoperable com-
13 munications.

14 (2) Issuing letters of intent to commit future
15 funds for jurisdictions through existing homeland se-
16 curity grant programs to applicants as appropriate
17 to encourage long-term investments that may signifi-
18 cantly improve communications interoperability.

19 (3) Providing technical assistance to additional
20 urban and other high-risk areas to support the es-
21 tablishment of consistent, secure, and effective inter-
22 operable communications capabilities.

23 (4) Completing the report to the Congress on
24 the Department's plans for accelerating the develop-
25 ment of national voluntary consensus standards for



1 public safety interoperable communications, a sched-
2 ule of milestones for such development, and achieve-
3 ments of such development, by no later than 30 days
4 after the date of enactment of this Act.

5 **SEC. 309. REPORT TO CONGRESS ON IMPLEMENTATION OF**
6 **RECOMMENDATIONS REGARDING PROTEC-**
7 **TION OF AGRICULTURE.**

8 The Secretary of Homeland Security shall report to
9 the appropriate congressional committees (as defined in
10 section 2 of the Homeland Security Act of 2002 (6 U.S.C.
11 101)) by no later than 120 days after the date of the en-
12 actment of this Act regarding how the Department of
13 Homeland Security will implement the applicable rec-
14 ommendations from the Government Accountability Office
15 report entitled "Homeland Security: Much is Being Done
16 to Protect Agriculture from a Terrorist Attack, but Impor-
17 tant Challenges Remain" (GAO-05-214).

18 **Subtitle B—Department of Home-**
19 **land Security Cybersecurity En-**
20 **hancement**

21 **SEC. 311. SHORT TITLE.**

22 This subtitle may be cited as the "Department of
23 Homeland Security Cybersecurity Enhancement Act of
24 2005".



1 **SEC. 312. ASSISTANT SECRETARY FOR CYBERSECURITY.**

2 Section 201(b) of the Homeland Security Act of 2002
3 (6 U.S.C. 121(b)) is amended—

4 (1) by redesignating paragraph (3) as para-
5 graph (4); and

6 (2) by inserting after paragraph (2) the fol-
7 lowing new paragraph:

8 “(3) ASSISTANT SECRETARY FOR
9 CYBERSECURITY.—There shall be in the Department
10 an Assistant Secretary for Cybersecurity, who shall
11 be appointed by the President.”; and

12 (3) in paragraph (4), as redesignated by sub-
13 paragraph (A) of this paragraph—

14 (A) by striking “Analysis and the” and in-
15 serting “Analysis, the”; and

16 (B) by striking “Protection shall” and in-
17 serting “Protection, and the Assistant Sec-
18 retary for Cybersecurity shall”.

19 **SEC. 313. CYBERSECURITY TRAINING PROGRAMS AND**
20 **EQUIPMENT.**

21 (a) **IN GENERAL.**—The Secretary of Homeland Secu-
22 rity, acting through the Assistant Secretary for
23 Cybersecurity, may establish, in conjunction with the Na-
24 tional Science Foundation, a program to award grants to
25 institutions of higher education (and consortia thereof)
26 for—



1 (1) the establishment or expansion of
2 cybersecurity professional development programs;

3 (2) the establishment or expansion of associate
4 degree programs in cybersecurity; and

5 (3) the purchase of equipment to provide train-
6 ing in cybersecurity for either professional develop-
7 ment programs or degree programs.

8 (b) ROLES.—

9 (1) DEPARTMENT OF HOMELAND SECURITY.—

10 The Secretary, acting through the Assistant Sec-
11 retary for Cybersecurity and in consultation with the
12 Director of the National Science Foundation, shall
13 establish the goals for the program established
14 under this section and the criteria for awarding
15 grants under the program.

16 (2) NATIONAL SCIENCE FOUNDATION.—The Di-
17 rector of the National Science Foundation shall op-
18 erate the program established under this section
19 consistent with the goals and criteria established
20 under paragraph (1), including soliciting applicants,
21 reviewing applications, and making and admin-
22 istering grant awards. The Director may consult
23 with the Assistant Secretary for Cybersecurity in se-
24 lecting awardees.



1 (3) FUNDING.—The Secretary shall transfer to
2 the National Science Foundation the funds nec-
3 essary to carry out this section.

4 (c) GRANT AWARDS.—

5 (1) PEER REVIEW.—All grant awards under
6 this section shall be made on a competitive, merit-
7 reviewed basis.

8 (2) FOCUS.—In making grant awards under
9 this section, the Director shall, to the extent prac-
10 ticable, ensure geographic diversity and the partici-
11 pation of women and underrepresented minorities.

12 (3) PREFERENCE.—In making grant awards
13 under this section, the Director shall give preference
14 to applications submitted by consortia of institutions
15 to encourage as many students and professionals as
16 possible to benefit from this program.

17 (d) AUTHORIZATION OF APPROPRIATIONS.—Of the
18 amount authorized under section 101, there is authorized
19 to be appropriated to the Secretary for carrying out this
20 section \$3,700,000 for fiscal year 2006.

21 (e) DEFINITIONS.—In this section, the term “institu-
22 tion of higher education” has the meaning given that term
23 in section 101(a) of the Higher Education Act of 1965
24 (20 U.S.C. 1001(a)).



1 **SEC. 314. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

2 Title III of the Homeland Security Act of 2002 (6
3 U.S.C. 181 et. seq.) is amended by adding at the end the
4 following new section:

5 **“SEC. 314. CYBERSECURITY RESEARCH AND DEVELOP-**
6 **MENT.**

7 “(a) IN GENERAL.—The Under Secretary for Science
8 and Technology shall support research and development,
9 including fundamental, long-term research, in
10 cybersecurity to improve the ability of the United States
11 to prevent, protect against, detect, respond to, and recover
12 from cyber attacks, with emphasis on research and devel-
13 opment relevant to large-scale, high-impact attacks.

14 “(b) ACTIVITIES.—The research and development
15 supported under subsection (a), shall include work to—

16 “(1) advance the development and accelerate
17 the deployment of more secure versions of funda-
18 mental Internet protocols and architectures, includ-
19 ing for the domain name system and routing proto-
20 cols;

21 “(2) improve and create technologies for detect-
22 ing attacks or intrusions, including monitoring tech-
23 nologies;

24 “(3) improve and create mitigation and recov-
25 ery methodologies, including techniques for contain-



1 ment of attacks and development of resilient net-
2 works and systems that degrade gracefully; and

3 “(4) develop and support infrastructure and
4 tools to support cybersecurity research and develop-
5 ment efforts, including modeling, testbeds, and data
6 sets for assessment of new cybersecurity tech-
7 nologies.

8 “(c) COORDINATION.—In carrying out this section,
9 the Under Secretary for Science and Technology shall co-
10 ordinate activities with—

11 “(1) the Assistant Secretary for Cybersecurity;
12 and

13 “(2) other Federal agencies, including the Na-
14 tional Science Foundation, the Defense Advanced
15 Research Projects Agency, and the National Insti-
16 tute of Standards and Technology, to identify unmet
17 needs and cooperatively support activities, as appro-
18 priate.

19 “(d) NATURE OF RESEARCH.—Activities under this
20 section shall be carried out in accordance with section
21 306(a) of this Act.”.



1 **Subtitle C—Security of Public**
2 **Transportation Systems**

3 **SEC. 321. SECURITY BEST PRACTICES.**

4 Not later than 120 days after the date of the enact-
5 ment of this Act, the Secretary of Homeland Security, in
6 coordination with the Secretary of Transportation, shall
7 issue a report containing best practices for the security
8 of public transportation systems related to the threats
9 from terrorism. Such report shall be developed in consulta-
10 tion with providers of public transportation, industry asso-
11 ciations, public transportation employee representatives,
12 first responders, and appropriate Federal, State, and local
13 officials. The Secretary of Transportation shall dissemi-
14 nate the report to providers of public transportation, in-
15 dustry associations, public transportation employee rep-
16 resentatives, and appropriate Federal, State, and local of-
17 ficials, the Committee on Homeland Security and the
18 Committee on Transportation and Infrastructure of the
19 House of Representatives, and any other appropriate enti-
20 ties.

21 **SEC. 322. PUBLIC AWARENESS.**

22 Not later than 90 days after the date of the enact-
23 ment of this Act, the Secretary of Transportation, after
24 consultation with the Secretary of Homeland Security,
25 shall develop a national plan to increase awareness of



1 measures that the general public, public transportation
2 passengers, and public transportation employees can take
3 to increase public transportation security related to the
4 threat of terrorism. Such plan shall also provide outreach
5 to providers and employees of public transportation sys-
6 tems on available transportation security technologies, on-
7 going research and development efforts, employee train-
8 ing, and available Federal funding sources to improve pub-
9 lic transportation security. Not later than 9 months after
10 the date of the enactment of this Act, the Secretary of
11 Transportation shall disseminate the plan to providers of
12 public transportation, industry associations, public trans-
13 portation employee representatives, appropriate Federal,
14 State, and local officials, and other appropriate entities.

15 **Subtitle D—Critical Infrastructure**
16 **Prioritization**

17 **SEC. 331. CRITICAL INFRASTRUCTURE.**

18 (a) **COMPLETION OF PRIORITIZATION.**—Not later
19 than 90 days after the date of the enactment of this Act,
20 the Secretary of Homeland Security shall complete the
21 prioritization of the Nation's critical infrastructure ac-
22 cording to all of the following criteria:

23 (1) The threat of terrorist attack, based on
24 threat information received and analyzed by the Of-
25 fice of Information Analysis of the Department re-



1 garding the intentions and capabilities of terrorist
2 groups and other potential threats to the Nation's
3 critical infrastructure.

4 (2) The likelihood that an attack would cause
5 the destruction or significant disruption of such in-
6 frastructure.

7 (3) The likelihood that an attack would result
8 in substantial numbers of deaths and serious bodily
9 injuries, a substantial adverse impact on the na-
10 tional economy, or a substantial adverse impact on
11 national security.

12 (b) COOPERATION.—Such prioritization shall be de-
13 veloped in cooperation with other relevant Federal agen-
14 cies, State, local, and tribal governments, and the private
15 sector, as appropriate.

16 **SEC. 332. SECURITY REVIEW.**

17 (a) REQUIREMENT.—Not later than 9 months after
18 the date of the enactment of this Act, the Secretary of
19 Homeland Security, in coordination with other relevant
20 Federal agencies, State, local, and tribal governments, and
21 the private sector, as appropriate, shall—

22 (1) review existing Federal, State, local, tribal,
23 and private sector plans for securing the critical in-
24 frastructure included in the prioritization developed
25 under section 331;



1 (2) recommend changes to existing plans for se-
2 curing such infrastructure, as the Secretary deter-
3 mines necessary; and

4 (3) coordinate and contribute to protective ef-
5 forts of other Federal, State, local, and tribal agen-
6 cies and the private sector, as appropriate.

7 (b) CONTENTS OF PLANS.—The recommendations
8 made under subsection (a)(2) shall include—

9 (1) protective measures to secure such infra-
10 structure, including milestones and timeframes for
11 implementation; and

12 (2) to the extent practicable, performance
13 metrics to evaluate the benefits to both national se-
14 curity and the Nation's economy from the implemen-
15 tation of such protective measures.

16 **SEC. 333. IMPLEMENTATION REPORT.**

17 (a) IN GENERAL.—Not later than 15 months after
18 the date of the enactment of this Act, the Secretary of
19 Homeland Security shall submit a report to the appro-
20 priate congressional committees (as defined in section 2
21 of the Homeland Security Act of 2002 (6 U.S.C. 101))
22 on the implementation of section 332. Such report shall
23 detail—

24 (1) the Secretary's review and coordination of
25 security plans under section 332; and



1 (2) the Secretary's oversight of the execution
2 and effectiveness of such plans.

3 (b) UPDATE.—Not later than 1 year after the sub-
4 mission of the report under subsection (a), the Secretary
5 shall provide an update of such report to the congressional
6 committees described in subsection (a).

7 **SEC. 334. PROTECTION OF INFORMATION.**

8 (a) PROTECTION OF INFORMATION.—The informa-
9 tion set forth in subsection (b) that is generated, compiled,
10 or disseminated by the Department of Homeland Security
11 in carrying out this subtitle—

12 (1) is exempt from disclosure under section 552
13 of title 5, United States Code; and

14 (2) shall not, if provided by the Department to
15 a State or local government or government agency—

16 (A) be made available pursuant to any
17 State or local law requiring disclosure of infor-
18 mation or records;

19 (B) otherwise be disclosed or distributed to
20 any person by such State or local government
21 or government agency without the written con-
22 sent of the Secretary; or

23 (C) be used other than for the purpose of
24 protecting critical infrastructure or protected



1 systems, or in furtherance of an investigation or
2 the prosecution of a criminal act.

3 (b) INFORMATION COVERED.—Information referred
4 to in subsection (a) is the following:

5 (1) The Secretary's prioritization of critical in-
6 frastructure pursuant to section 331, including any
7 information upon which such prioritization was
8 based;

9 (2) the Secretary's review of existing security
10 plans for such infrastructure pursuant to section
11 332(a)(1).

12 (3) The Secretary's recommendations for
13 changes to existing plans for securing such infra-
14 structure pursuant to section 332(a)(2).

15 (4) The nature and scope of protective efforts
16 with respect to such infrastructure under section
17 332(a)(3).

18 (5) The report and update prepared by the Sec-
19 retary pursuant to section 333, including any infor-
20 mation upon which such report and update are
21 based.



1 **TITLE IV—U.S. CUSTOMS AND**
2 **BORDER PROTECTION AND**
3 **U.S. IMMIGRATION AND CUS-**
4 **TOMS ENFORCEMENT**

5 **SEC. 401. ESTABLISHMENT AND IMPLEMENTATION OF**
6 **COST ACCOUNTING SYSTEM; REPORTS.**

7 Section 334 of the Customs and Border Security Act
8 of 2002 (19 U.S.C. 2082 note) is amended to read as fol-
9 lows:

10 **“SEC. 334. ESTABLISHMENT AND IMPLEMENTATION OF**
11 **COST ACCOUNTING SYSTEM; REPORTS.**

12 **“(a) ESTABLISHMENT AND IMPLEMENTATION; CUS-**
13 **TOMS AND BORDER PROTECTION.—**

14 **“(1) IN GENERAL.—**Not later than September
15 30, 2006, the Commissioner of U.S. Customs and
16 Border Protection shall, in accordance with the
17 audit of the Customs Service’s fiscal years 2000 and
18 1999 financial statements (as contained in the re-
19 port of the Office of Inspector General of the De-
20 partment of the Treasury issued on February 23,
21 2001), establish and implement a cost accounting
22 system—

23 **“(A) for expenses incurred in both com-**
24 **mercial and noncommercial operations of U.S.**
25 **Customs and Border Protection of the Depart-**



1 ment of Homeland Security, which system
2 should specifically identify and distinguish ex-
3 penses incurred in commercial operations and
4 expenses incurred in noncommercial operations;
5 and

6 “(B) for expenses incurred both in admin-
7 istering and enforcing the customs laws of the
8 United States and the Federal immigration
9 laws, which system should specifically identify
10 and distinguish expenses incurred in admin-
11 istering and enforcing the customs laws of the
12 United States and the expenses incurred in ad-
13 ministering and enforcing the Federal immigra-
14 tion laws.

15 “(2) ADDITIONAL REQUIREMENT.—The cost ac-
16 counting system described in paragraph (1) shall
17 provide for an identification of expenses based on
18 the type of operation, the port at which the oper-
19 ation took place, the amount of time spent on the
20 operation by personnel of U.S. Customs and Border
21 Protection, and an identification of expenses based
22 on any other appropriate classification necessary to
23 provide for an accurate and complete accounting of
24 expenses.



1 “(b) ESTABLISHMENT AND IMPLEMENTATION; IMMI-
2 GRATION AND CUSTOMS ENFORCEMENT.—

3 “(1) IN GENERAL.—Not later than September
4 30, 2006, the Assistant Secretary for U.S. Immigra-
5 tion and Customs Enforcement shall, in accordance
6 with the audit of the Customs Service’s fiscal years
7 2000 and 1999 financial statements (as contained in
8 the report of the Office of Inspector General of the
9 Department of the Treasury issued on February 23,
10 2001), establish and implement a cost accounting
11 system—

12 “(A) for expenses incurred in both com-
13 mercial and noncommercial operations of U.S.
14 Immigration and Customs Enforcement of the
15 Department of Homeland Security, which sys-
16 tem should specifically identify and distinguish
17 expenses incurred in commercial operations and
18 expenses incurred in noncommercial operations;

19 “(B) for expenses incurred both in admin-
20 istering and enforcing the customs laws of the
21 United States and the Federal immigration
22 laws, which system should specifically identify
23 and distinguish expenses incurred in admin-
24 istering and enforcing the customs laws of the
25 United States and the expenses incurred in ad-



1 ministering and enforcing the Federal immigra-
2 tion laws.

3 “(2) ADDITIONAL REQUIREMENT.—The cost ac-
4 counting system described in paragraph (1) shall
5 provide for an identification of expenses based on
6 the type of operation, the amount of time spent on
7 the operation by personnel of U.S. Immigration and
8 Customs Enforcement, and an identification of ex-
9 penses based on any other appropriate classification
10 necessary to provide for an accurate and complete
11 accounting of expenses.

12 “(c) REPORTS.—

13 “(1) DEVELOPMENT OF THE COST ACCOUNTING
14 SYSTEMS.—Beginning on the date of the enactment
15 of the Department of Homeland Security Authoriza-
16 tion Act for Fiscal Year 2006 and ending on the
17 date on which the cost accounting systems described
18 in subsections (a) and (b) are fully implemented, the
19 Commissioner of U.S. Customs and Border Protec-
20 tion and the Assistant Secretary for U.S. Immigra-
21 tion and Customs Enforcement, respectively, shall
22 prepare and submit to Congress on a quarterly basis
23 a report on the progress of implementing the cost
24 accounting systems pursuant to subsections (a) and
25 (b).



1 “(2) ANNUAL REPORTS.—Beginning one year
2 after the date on which the cost accounting systems
3 described in subsections (a) and (b) are fully imple-
4 mented, the Commissioner of U.S. Customs and
5 Border Protection and the Assistant Secretary for
6 U.S. Immigration and Customs Enforcement, re-
7 spectively, shall prepare and submit to Congress on
8 an annual basis a report itemizing the expenses
9 identified in subsections (a) and (b).

10 “(3) OFFICE OF THE INSPECTOR GENERAL.—
11 Not later than March 31, 2007, the Inspector Gen-
12 eral of the Department of Homeland Security shall
13 prepare and submit to Congress a report analyzing
14 the level of compliance with this section and detail-
15 ing any additional steps that should be taken to im-
16 prove compliance with this section.”.

17 **SEC. 402. REPORT RELATING TO ONE FACE AT THE BOR-**
18 **DER INITIATIVE.**

19 Not later than September 30 of each of the calendar
20 years 2006 and 2007, the Commissioner of U.S. Customs
21 and Border Protection of the Department of Homeland
22 Security shall prepare and submit to Congress a report—

23 (1) analyzing the effectiveness of the One Face
24 at the Border Initiative at enhancing security and
25 facilitating trade;



1 (2) providing a breakdown of the number of
2 personnel of U.S. Customs and Border Protection
3 that were personnel of the United States Customs
4 Service prior to the establishment of the Department
5 of Homeland Security, that were personnel of the
6 Immigration and Naturalization Service prior to the
7 establishment of the Department of Homeland Secu-
8 rity, and that were hired after the establishment of
9 the Department of Homeland Security;

10 (3) describing the training time provided to
11 each employee on an annual basis for the various
12 training components of the One Face at the Border
13 Initiative; and

14 (4) outlining the steps taken by U.S. Customs
15 and Border Protection to ensure that expertise is re-
16 tained with respect to customs, immigration, and ag-
17 riculture inspection functions under the One Face at
18 the Border Initiative.

19 **SEC. 403. CUSTOMS SERVICES.**

20 Section 13031(e)(1) of the Consolidated Omnibus
21 Budget Reconciliation Act of 1985 (19 U.S.C. 58c(e)(1))
22 is amended—

23 (1) by striking “(1) Notwithstanding section
24 451 of the Tariff Act of 1930 (19 U.S.C. 1451) or



1 any other provision of law (other than paragraph
2 (2)),” and inserting:

3 “(1) IN GENERAL.—

4 “(A) SCHEDULED FLIGHTS.—Notwith-
5 standing section 451 of the Tariff Act of 1930
6 (19 U.S.C. 1451) or any other provision of law
7 (other than subparagraph (B) and paragraph
8 (2)),”; and
9 (2) by adding at the end the following:

10 “(B) CHARTER FLIGHTS.—If a charter air
11 carrier (as defined in section 40102(13) of title
12 49, United States Code) specifically requests
13 that customs border patrol services for pas-
14 sengers and their baggage be provided for a
15 charter flight arriving after normal operating
16 hours at a customs border patrol serviced air-
17 port and overtime funds for those services are
18 not available, the appropriate customs border
19 patrol officer may assign sufficient customs em-
20 ployees (if available) to perform any such serv-
21 ices, which could lawfully be performed during
22 regular hours of operation, and any overtime
23 fees incurred in connection with such service
24 shall be paid by the charter air carrier.”.



1 **SEC. 404. SENSE OF CONGRESS ON INTERPRETATION OF**
2 **TEXTILE AND APPAREL PROVISIONS.**

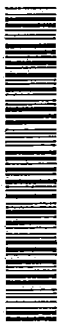
3 It is the sense of Congress that U.S. Customs and
4 Border Protection of the Department of Homeland Secu-
5 rity should interpret, implement, and enforce the provi-
6 sions of section 112 of the African Growth and Oppor-
7 tunity Act (19 U.S.C. 3721), section 204 of the Andean
8 Trade Preference Act (19 U.S.C. 3203), and section 213
9 of the Caribbean Basin Economic Recovery Act (19
10 U.S.C. 2703), relating to preferential treatment of textile
11 and apparel articles, broadly in order to expand trade by
12 maximizing opportunities for imports of such articles from
13 eligible beneficiary countries.

14 **TITLE V—MISCELLANEOUS**

15 **SEC. 501. BORDER SECURITY AND ENFORCEMENT COORDI-**
16 **NATION AND OPERATIONS.**

17 (a) FINDINGS.—The Congress makes the following
18 findings:

19 (1) As part of the creation of the Department
20 of Homeland Security, section 442 of the Homeland
21 Security Act of 2002 (Public Law 107–273) estab-
22 lished a Bureau of Border Security and transferred
23 into it all of the functions, programs, personnel, as-
24 sets, and liabilities pertaining to the following pro-
25 grams: the Border Patrol; alien detention and re-
26 moval; immigration-related intelligence, investiga-



1 tions, and enforcement activities; and immigration
2 inspections at ports of entry.

3 (2) Title IV of the Homeland Security Act of
4 2002 (Public Law 107-273) also transferred to the
5 new Department the United States Customs Service,
6 as a distinct entity within the new Department, to
7 further the Department's border integrity mission.

8 (3) Utilizing its reorganization authority pro-
9 vided in the Homeland Security Act of 2002, the
10 President submitted a reorganization plan for the
11 Department on January 30, 2003.

12 (4) This plan merged the customs and immigra-
13 tion border inspection and patrol functions, along
14 with agricultural inspections functions, into a new
15 entity called United States Customs and Border
16 Protection.

17 (5) The plan also combined the customs and
18 immigration enforcement agents, as well as the Of-
19 fice of Detention and Removal Operations, the Of-
20 fice of Federal Protective Service, the Office of Fed-
21 eral Air Marshal Service, and the Office of Intel-
22 ligence, into another new entity called United States
23 Immigration and Customs Enforcement.

24 (6) The President's January 30, 2003, reorga-
25 nization plan did not explain the reasons for sepa-



1 rating immigration inspection and border patrol
2 functions from other immigration-related enforce-
3 ment functions, or to combine immigration-related
4 enforcement functions with customs and other func-
5 tions, contrary to the design of the Bureau of Bor-
6 der Security as prescribed by the Congress in section
7 442 of the Homeland Security Act of 2002.

8 (7) United States Immigration and Customs
9 Enforcement has faced major budgetary challenges
10 that are, in part, attributable to the inexact division
11 of resources upon the separation of immigration
12 functions. These budget shortfalls have forced
13 United States Immigration and Customs Enforce-
14 ment to impose hiring freezes and to release aliens
15 that otherwise should be detained.

16 (b) REPORT.—

17 (1) IN GENERAL.—Not later than 30 days after
18 the date of the enactment of this Act, the Secretary
19 of Homeland Security shall review and evaluate the
20 current organizational structure of the Department
21 of Homeland Security established by the President's
22 January 30, 2003, reorganization plan and submit a
23 report of findings and recommendations to the ap-
24 propriate congressional committees (as defined in



1 section 2 of the Homeland Security Act of 2002 (6
2 U.S.C. 101)).

3 (2) CONTENTS OF REPORT.—The report shall
4 include—

5 (A) a description of the rationale for, and
6 any benefits of, the current organizational divi-
7 sion of United States Immigration and Customs
8 Enforcement and United States Customs and
9 Border Protection, with respect to the Depart-
10 ment's immigration and customs missions;

11 (B) a description of the organization, mis-
12 sions, operations, and policies of United States
13 Customs and Border Protection and United
14 States Immigration and Customs Enforcement,
15 and areas of unnecessary overlap or operational
16 gaps among and between these missions;

17 (C) a description of the rationale for, and
18 any benefits of, the current organizational com-
19 bination of immigration-related enforcement
20 functions with customs and other functions;

21 (D) an analysis of alternative organiza-
22 tional structures that could provide a more ef-
23 fective way to deliver maximum efficiencies and
24 mission success;



1 (E) a description of the current role of the
2 Directorate of Border and Transportation Secu-
3 rity with respect to providing adequate direction
4 and oversight of the two agencies, and whether
5 this management structure is still necessary;

6 (F) an analysis of whether the Federal Air
7 Marshals and the Federal Protective Service are
8 properly located within the Department within
9 United States Immigration and Customs En-
10 forcement;

11 (G) the proper placement and functions of
12 a specialized investigative and patrol unit oper-
13 ating at the southwest border on the Tohono
14 O'odham Nation, known as the Shadow Wolves;

15 (H) the potential costs of reorganization,
16 including financial, programmatic, and other
17 costs, to the Department; and

18 (I) recommendations for correcting the
19 operational and administrative problems that
20 have been caused by the division of United
21 States Custom and Border Protection and
22 United States Immigration and Customs En-
23 forcement and by the combination of immigra-
24 tion-related enforcement functions with customs



1 and other functions in both entities, including
2 any appropriate reorganization plans.

3 **SEC. 502. GAO REPORT TO CONGRESS.**

4 (a) IN GENERAL.— Not later than 6 months after
5 the date of the enactment of this Act, the Comptroller
6 General of the United States shall submit to the appro-
7 priate congressional committees (as defined in section 2
8 of the Homeland Security Act of 2002 (6 U.S.C. 101))
9 a report that sets forth—

10 (1) an assessment of the effectiveness of the or-
11 ganizational and management structure of the De-
12 partment of Homeland Security in meeting the De-
13 partment's missions as set forth in section 101(b)(1)
14 of the Homeland Security Act of 2002 (6 U.S.C.
15 111(b)(1)); and

16 (2) recommendations to facilitate and improve
17 the organization and management of the Depart-
18 ment to best meet those missions.

19 (b) CYBERSECURITY ASSESSMENT.—Not later than
20 one year after the date of the enactment of this Act, the
21 Comptroller General shall submit a report to the appro-
22 priate congressional committees (as defined in section 2
23 of the Homeland Security Act of 2002 (6 U.S.C. 101))
24 that sets forth an assessment of the effectiveness of the



1 efforts of the Assistant Secretary for Cybersecurity to ful-
2 fill the statutory responsibilities of that office.

3 **SEC. 503. PLAN TO REDUCE WAIT TIMES.**

4 Not later than 180 days after the date of enactment
5 of this Act, the Secretary of Homeland Security shall de-
6 velop a plan—

7 (1) to improve the operational efficiency of se-
8 curity screening checkpoints at commercial service
9 airports so that average peak waiting periods at
10 such checkpoints do not exceed 20 minutes; and

11 (2) to ensure that there are no significant dis-
12 parities in immigration and customs passenger proc-
13 essing times among airports that serve as inter-
14 national gateways.

15 **SEC. 504. DENIAL OF TRANSPORTATION SECURITY CARD.**

16 Section 70105(c) of title 46, United States Code, is
17 amended—

18 (1) in paragraph (3) by inserting before the pe-
19 riod “before an administrative law judge”; and

20 (2) by adding at the end the following:

21 “(5) In making a determination under paragraph
22 (1)(D) that an individual poses a terrorism security risk,
23 the Secretary shall not solely consider a felony conviction
24 if—



1 “(A) that felony occurred more than 7 years
2 prior to the date of the Secretary’s determination;
3 and

4 “(B) the felony was not related to terrorism (as
5 that term is defined in section 2 of the Homeland
6 Security Act of 2002 (6 U.S.C. 101)).”.

7 **SEC. 505. TRANSFER OF EXISTING CUSTOMS PATROL OFFI-**
8 **CERS UNIT AND ESTABLISHMENT OF NEW**
9 **CPO UNITS IN THE BUREAU OF IMMIGRATION**
10 **AND CUSTOMS ENFORCEMENT.**

11 (a) **TRANSFER OF EXISTING UNIT.**—Not later than
12 180 days after the date of the enactment of this Act, the
13 Secretary of Homeland Security shall transfer to the Bu-
14 reau of Immigration and Customs Enforcement all func-
15 tions (including the personnel, assets, and obligations held
16 by or available in connection with such functions) of the
17 Customs Patrol Officers unit of the Bureau of Customs
18 and Border Protection operating on the Tohono O’odham
19 Indian reservation (commonly known as the ‘Shadow
20 Wolves’ unit).

21 (b) **ESTABLISHMENT OF NEW UNITS.**—The Sec-
22 retary is authorized to establish within the Bureau of Im-
23 migration and Customs Enforcement additional units of
24 Customs Patrol Officers in accordance with this section.



1 (c) DUTIES.—The Customs Patrol Officer unit trans-
2 ferred pursuant to subsection (a) and the additional units
3 established pursuant to subsection (b) shall be responsible
4 for the prevention of the smuggling of narcotics, weapons
5 of mass destruction, and other contraband, and the illegal
6 trafficking of persons, on Indian lands.

7 (d) BASIC PAY FOR JOURNEYMAN OFFICERS.—A
8 Customs Patrol Officer in a unit described in this section
9 shall receive equivalent pay as a special agent with similar
10 competencies within the Bureau of Immigration and Cus-
11 toms Enforcement pursuant to the Department of Home-
12 land Security's human resources management system es-
13 tablished under section 841 of the Homeland Security Act
14 (6 U.S.C. 411).

15 (e) SUPERVISORS.—Each unit described under this
16 section shall be supervised by a Chief Customs Patrol Offi-
17 cer, who shall have the same rank as a resident agent-
18 in-charge of the Office of Investigations.

19 **SEC. 506. DATA COLLECTION ON USE OF IMMIGRATION**
20 **CONSULTANTS.**

21 The Secretary of Homeland Security shall establish
22 procedures to record information on applications for an
23 immigration benefit submitted by an alien with respect to
24 which—



1 (1) the alien states that the alien used the serv-
2 ices of an immigration consultant; or

3 (2) a Department employee or official inves-
4 tigating facts alleged in the application, or adjudi-
5 cating the application, suspects that the alien used
6 the services of an immigration consultant.

7 **SEC. 507. OFFICE FOR STATE AND LOCAL GOVERNMENT**
8 **COORDINATION.**

9 The Homeland Security Act of 2002 is amended—
10 (1) in section 801—

11 (A) in the section heading, by striking
12 “**STATE AND LOCAL**” and inserting “**STATE,**
13 **LOCAL, AND TRIBAL**”;

14 (B) in subsection (a), by striking “State
15 and Local” and inserting “State, Local, and
16 Tribal”; and

17 (C) in subsection (b), by striking “State
18 and local” each place it appears and inserting
19 “State, local, and tribal”; and

20 (2) in section 1(b) in the table of contents by
21 striking the item relating to section 801 and insert-
22 ing the following:

“Sec. 801. Office for State, Local, and Tribal Government Coordination.”.



1 **SEC. 508. AUTHORITY OF OTHER FEDERAL AGENCIES UN-**
2 **AFFECTED.**

3 Except to the extent explicitly provided in section
4 216, nothing in this Act shall affect the authority under
5 statute, regulation, or Executive order of other Federal
6 agencies than the Department of Homeland Security.

